NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer
P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212
www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 116 – Security Assessment Policy	**POLICY NO:** 14-14-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 07/28/2014
	VERSION: 1.0	**LAST REVIEWED:** 07/28/2014

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this policy is to ensure the implementation of the appropriate security controls, both technical and non-technical, across the Executive Branch of State government. The Office of Information Technology maintains oversight of the security controls necessary to ensure the confidentiality, integrity, and availability of those information technology assets and resources within New Jersey's Executive Branch of State Government, and oversees the network linking State computing systems.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This policy defines the New Jersey Office of Information Technology's (NJOIT) role with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

3 SCOPE

This policy applies to all State of New Jersey systems and equipment that process, transmit, or store State of New Jersey information. This policy applies to all state departments, agencies, "in but not of" entities, their employees, contractors, consultants, temporary workers, and others who develop and administer information systems and resources for systems.

4 POLICY

A Security Assessment is focused on determining the degree to which security controls are correctly implemented, whether they are operating as intended, and if they are producing the desired level of security protection. Without Security Assessments information systems may be at risk from cyber-attacks or security data breaches.

This policy establishes that the Statewide Information Security Officer (SISO) and the Statewide Office of Information Security (SOIS) are responsible for directing the security assessment standards for state information technology assets.

4.1.1 The Security Assessment will establish and ensure that:

4.1.2 Information technology assets to be assessed are defined and documented by the agency or asset owner.

4.1.3 Assessments will be performed during each phase of the System Development Life Cycle (SDLC).

4.1.4 Physical, technical, and administrative security controls, as specified in *14-01-S1-NJOIT 171-01 Minimum System Security Requirements Standards* (*This standard is published/posted in NJ-ISAC),* are assessed as to their capability to protect the information and resources within the state.

4.1.5 Assessments will be performed by reviewing documentation and interviewing system administrators, security officers, and system owners.

4.1.6 Risks will be identified and plans will be established to address and mitigate any weaknesses through action plans as specified in 14-02-NJOIT, *115-Information Security Risk Management Policy*. Information technology assets 'risks should be reported and remediated as soon as possible until completion or an exception has been authorized.

4.1.7 Information technology assets will be reassessed whenever there is a major change in a system during a System Architecture Review.

5 RESPONSIBILITIES

5.1.1 Statewide Information Security Officer and Statewide Office of Information Security

The SISO and SOIS are responsible for overseeing the Security Assessments of information technology assets while performing the following duties:

5.1.1.1 Administering the security assessment process and periodically evaluating whether the program is implemented effectively.

5.1.1.2 Conducting assessments during each phase of the System Development Life Cycle (SDLC).

5.1.1.3 Developing and implementing security policies, standards and procedures.

5.1.1.4 Reviewing requested exceptions to security policies, standards and procedures.

5.1.1.5 Providing solutions, guidance and expertise in IT security remediation of security risks and vulnerabilities.

5.1.1.6 Maintaining awareness of security status of the information assets.

5.1.2 Agencies

Each Agency is responsible for the protection of its information assets from unauthorized disclosure, loss, or misuse. As such, each agency must maintain a thorough knowledge of and document the necessary security controls to protect these information assets.

Each Agency is responsible to identify known risks, provide a mitigation strategy, remediate and reporting them to business owners and SOIS.

Each Agency is responsible to work with SOIS in the completion of the security assessment.

6 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and non-compliance with this policy shall be managed in accordance with OIT Policy *08-02-NJOIT (111 – Information Security Managing Exceptions)*.